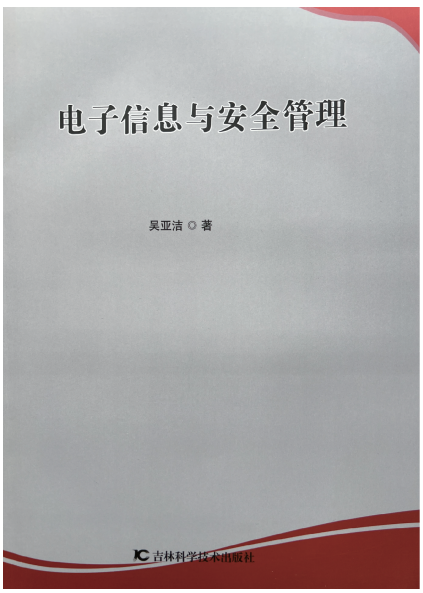
智能化时代电子信息安全管理策略
——评《电子信息与安全管理》

在数字化浪潮席卷全球的今天,智能化时代的电子信息安全,绝不仅仅是技术的堆砌,而是一场涉及意识、制度与技术的深刻变革。必须摒弃侥幸心理,以雷霆手段构建立体电子信息安全防护体系,实施全生命周期的智能主动防御策略。

笔者在开展2024年山东省职业教育教学改革研究项目(2024425)研究过程中,认真阅读了《电子信息与安全管理》一书,该书并未局限于单纯技术探讨,而倾向于搭建一座连接电子信息技术底层逻辑与金融支付实务的桥梁。全书以电子支付体系为核心,既深度全面系统梳理了从传统支付工具到网络银行、第三方结算及移动支付的演变脉络,又将视角延伸至金融科技前沿。对于"安全"的探讨尤为务实,跳出了纯技术参数窠臼,结合具体业务场景分析了支付信息安全的防护策略,通过深入浅出解读,让读者真正理解了现代支付系统底座运行的逻辑。



书名:电子信息与安全管理
作者:吴亚洁
出版社:吉林科学技术出版社
ISBN:9787574412361
出版时间:2024年3月
定价:70元

该书作者指出,传统的"边界防御"模式,即筑起高墙、区分内外,在云计算、移动办公和物联网泛滥的今天已彻底失效。内部人员可能被收买,外部攻击者可能早已潜伏在内网。因此,必须确立"永不信任,始终验证"的铁律,将安全管理从"网络位置"转向"身份与行为"。首先,实施颗粒度极细的访问控制。绝不能搞"一刀切"的权限分配,而要基于用户角色、设备状态、时间地点乃至行为特征进行动态授权。如智能电网的安全防护原则,必须将实时控制区与管理信息区进行物理级的逻辑隔离,利用纵向加密、横向隔离技术,确保即便攻击者突破了外层防线,也无法触及核心业务系统。对于涉及国家秘密、核心技术图纸等高度敏感信息的岗位,必须执行"最小必要原则",甚至直接禁止外部人工智能(Artificial Intelligence,AI)工具的访问,仅允许在物理隔离的内部智能系统中操作。其次,建立全生命周期的身份认证体系。身份是零信任的基石,要推进国家网络身份认证公共服务的落地,利用"网证网号+动态认证"切断互联网平台对原始身份信息的直接接触,从源头上杜绝个人信息泄露的"木桶短板"。即便是企业内部管理中,亦有必要结合多因素认证技术与单点登录要求,从登录源头确保每一次登录访问都是被授权的,且登录人是权限授予人。最后,主动推行未隔离技术与流量数据加密技术,尤其是对于金融等核心敏感数据传输,传输过程中要经过防火墙,并对数据进行深度清洗和高强度加密,确保不会出现被截获破解的风险。

笔者认为,随着AI技术持续进化更新,部分意图不当的机构与个人利用AI技术自动挖掘漏洞,并籍此进行攻击,或利用AI技术生成病毒变种,提高攻击效率,防不胜防。面对传统病毒监测工具由AI技术生成病毒的防御效果不佳的现实情况,安全技术人员亦应主动利用AI技术构建主动智能防御体系,相对于人工解析风险,AI解析更全面,既可降低成本,也可提高效率。企业与技术员通过引入专业级的AI安全模型,其基于大数据分析技术实时全量监控海量网络流量。AI模型能通过异常行为分析,精准识别未知的零日攻击和隐蔽的后门通信,如通过分析电力负荷控制系统的微小波动或金融交易的异常流向,AI安全模型可在攻击造成实质破坏前发出预警,并自动触发阻断机制,给专业人员介入风控争取更多安全时间。与此同时,从事安全技术企业和AI系统使用人员须严控AI使用边界,构建数据防泄漏的"隔离网"。AI工具应用日趋广泛,其便捷性往往让人忽视其背后的数据吞噬风险,企业或个人每输入AI的每一段文字、每一张图片,都可能成为训练语料并被关联分析,导致"拼图式泄密",基于此,有必要建立严格的AI使用分级授权体系和行为审计平台。企业应部署数据防泄漏系统和AI使用行为审计系统,对上传至外部AI平台的文件进行实时拦截,对敏感字段进行自动脱敏——如将真实姓名替换为代号,将精确金额模糊为区间,删减核心算法参数,降低风险隐患。

总之,电子信息安全管理绝非一劳永逸的工程,而是一场没有硝烟的持久战。在这场博弈中,技术是盾,管理是柄,意识是魂。通过"零信任"架构重塑信任链条,利用AI技术赋能主动防御,并辅以严苛的数据治理与合规体系,方能在数字化的惊涛骇浪中稳住舵盘。

(董建民/山东工业职业学院电气工程学院/副教授)